(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 October 2001 (25.10.2001)

PCT

(10) International Publication Number
WO 01/78491 A2

(51) International Patent Classification: Not classified

(21) International Application Number: PCT/US01/12157

(22) International Filing Date: 12 April 2001 (12.04.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/549,446 14 April 2000 (14.04.2000) US

(71) Applicant: **POSTX CORPORATION** [US/US]; 3 Results Way, Cupertino, CA 95014 (US).

(72) Inventors: **VENKATRAMAN, Rajamadam, C.**; 1031 Harlan Drive, San Jose, CA 95129 (US). **SAHASRABAUDDHE, Unmesh**; 875 University Avenue #5, Palo Alto, CA 94301 (US). **SHORT, Steven**; 786 Bend Avenue, San Jose, CA 95136 (US). **WARTY, Ashish**; 1818 Canal Way, San Jose, CA 95132 (US).

(74) Agents: **JAKOPIN, David, A.** et al.; Pillsbury Winthrop LLP, 1100 New York Avenue, N.W., Washington, DC 20005 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 01/78491 A2

(54) Title: SYSTEMS AND METHODS FOR ENCRYPTING/DECRYPTING DATA

(57) Abstract: The present invention relates to systems and methods for providing secure symmetric and asymmetric encryption/decryption using an intermediate or broker agent. The present systems and methods provide a more advanced and sophisticated manner of preventing unauthorized users from accessing sensitive and private data that is transmitted via the Internet. The broker agent (i.e., a server) is used to encrypt and decrypt data and/or session key during the transmission of the data from the sender to the recipient. These encryption processes are more secure because the recipients do not have access to the sender's private and public keys. The first and second embodiment relate to symmetric encryption/decryption systems and methods, while the third and fourth embodiments relate to asymmetric encryption/decryption systems and methods.

DE

SYSTEMS AND METHODS FOR ENCRYPTING/DECRYPTING DATA

FIELD OF THE INVENTION

The present invention relates to the field of security and privacy on a distributed communication system such as the Internet. More particularly, the present invention is directed to systems and methods for encrypting/decrypting data in electronic documents and messages using an intermediate or broker agent.

BACKGROUND OF THE INVENTION

Exchanging information using a distributed communication system such as the Internet continues to gain in popularity among individual users and businesses in the current information age. It is of no surprise that the Internet is the preferred method of transmitting/receiving documents, messages, mail, and the like.

There are many advantages of using the Internet for transmitting/receiving documents, messages, and the like. For example, when a sender transmits an email to a recipient, the recipient typically receives the email in a matter of seconds or minutes, depending on the location of the sender and the recipient. The ability to instantaneously exchange information from one person to another is one of the most beneficial aspects of the Internet. In addition, documents, messages, mail, and the like can be transmitted from one person to another with minimal costs. There are typically no shipping costs such as postage, envelopes, paper, etc., associated with transmitting documents and messages via the Internet.

The Internet is generally designed to allow for the freest possible exchange of information, data, files, etc. When data travels via the Internet, it typically passes through many computer systems and networks before arriving at its destination. As a result, other Internet users besides the intended recipient(s) may be able to intercept the data and view it without authorization.

As people and businesses use the Internet for transmitting and receiving information/data more frequently, more and more sensitive and private information is transmitted. For example, it is well known that many commercial banks transmit confidential account information electronically to their customers. In this manner, customers can view their bank statements, cancelled checks, etc., using their personal computer system. In another example, users may transmit sensitive and confidential materials such as personal credit card numbers, social security number, legal documents, etc., over the Internet. Also, many people are using the Internet as a preferred method for purchasing goods and services, trading stocks, applying for loans and credit cards, and the like.

Most data transmitted over the Internet are unsecured. As a consequence, various tools have been developed to make such transmissions more secure and private. For example, secure sockets layer (SSL) and various encryption/decryption methods have been developed to prevent unauthorized users from viewing the sensitive and private data.

Encryption is basically a technique used to transform data into a form unreadable by anyone without a secret decryption key. The general concept behind the conventional encryption-decryption method is that when the sender encrypts the data with a key, then only someone else with the matching key will be able to decrypt the data.

Fig. 1A illustrates a conventional symmetric encryption/decryption system having a sender's computer system and a recipient's computer system. In the conventional symmetric system, the sender's computer system 2 and the recipient's computer system 12 generally include and/or have access to a mutually agreed security key 6. Thus, each party (sender and recipient) has access to the security key 6 that both parties have previously agreed to share and implement. The two computer systems 2, 12 communicate with each other via a distributed communication system, e.g., Internet 18.

Fig. 1B illustrates a flow chart of a conventional symmetric encryption/decryption method for encrypting/decrypting data using the system of Fig. 1A. Reference will be made concurrently to Figs. 1A and 1B for a more complete understanding of the conventional symmetric encryption/decryption method. During operation, the sender encrypts the data at the sender's system 2 using the mutually agreed security key 6 in step 20. That is, the sender alters the information so that it will look like meaningless garble of data to anyone other than the intended recipient.

The encrypted data is then transmitted to the recipient's system 12 via the Internet 18 in step 22, and the recipient's system 12 receives the encrypted data in step 24. The recipient 12 next decrypts the data using the mutually agreed security key 6 in step 26 so that the data can be turned back into its original form.

In a similar manner as described above, the recipient's system 12 can send data encrypted using the mutually agreed security key 6 to the sender's system 2. The sender's system 2 can then decrypt the data using the mutually agreed security key 6 stored or retrieved therein.

Fig. 2A illustrates a conventional asymmetric encryption/decryption system having a sender's computer system and a recipient's computer system. In the conventional asymmetric system, the sender's computer system 2 includes and/or has access to a sender's private key 4, sender's public key 7, and recipient's public key 8. Likewise, the recipient's computer system 12 includes and/or has access to a recipient's private key 10, sender's public key 7, and recipient's public key 8. Thus, each party (sender and recipient) can access both private and public keys via its computer system or from some other

location on the Internet/World Wide Web (WWW). Each private key is kept secret and is known only by its owner, whereas the public keys for both the sender and the recipient are known to each other. In other words, the sender's private key 4 is known only to the sender's system 2, and the recipient's private key 10 is known only to the recipient's system 12. The sender's public key 7 and the recipient's public key 8 are known to both the sender's system 2 and the recipient's system 12. Again, the two computer systems 2, 12 communicate with each other via the Internet 18.

Fig. 2B illustrates a flow chart of a conventional asymmetric encryption/decryption method for encrypting/decrypting data using the system of Fig. 2A. Reference will be made concurrently to Figs. 2A and 2B for a more complete understanding of the conventional asymmetric encryption/decryption method. During operation, the sender encrypts the data at the sender's system 2 using the recipient's public key 8 in step 30. The encrypted data is then transmitted to the recipient's system 12 via the Internet 18 in step 32, and the recipient's system 12 receives the encrypted data in step 34. The recipient 12 next decrypts the data using the recipient's private key 10 in step 36 so that the data can be turned back into its original form.

In a similar manner as described above, the recipient's system 12 can send data encrypted using the sender's public key 7 to the sender's system 2. The sender's system 2 can then decrypt the data using the sender's private key 4.

The conventional symmetric and asymmetric encryption systems and methods described above allow the sender and the recipient to exchange data securely using security keys. The sender of the data encrypts it using the mutually agreed key or recipient's public key, and the recipient decrypts it using the mutually agreed key or recipient's private key. An important aspect of the conventional encryption is that data encrypted using the mutually agreed/public key of the recipient can only be decrypted using the mutually agreed/private key of the recipient. Thus, a major shortcoming of the conventional systems and methods are that the sender must know the public key of the recipient in order to encrypt the data. Accordingly, there is a need for systems and methods for providing a more advanced and sophisticated manner of encryption/decryption.

SUMMARY OF THE INVENTION

In view of the above-described problems of the prior art, it is an object of the present invention to provide a system and method for generating secure asymmetric and symmetric encryption/decryption.

It is another object of the present invention to provide a secure method of transmitting sensitive and private data via the Internet.

It is yet another object of the present invention to provide a secure method of transmitting sensitive

and private data via the Internet using an intermediate or broker agent.

It is a further object of the present invention to provide a method for encrypting and decrypting data using one user's key without knowledge of the other user's key.

It is another object of the present invention to provide a method for encrypting and decrypting data using a session key.

It is yet another object of the present invention to provide a method for encrypting and decrypting session keys that are used to encrypt and decrypt the data.

These and other objects of the present invention are obtained by providing systems and methods for generating secure symmetric and asymmetric encryption/decryption. An intermediate or broker agent is used for providing encryption/decryption between the sender and the recipient. In other words, a trusted third party, i.e., broker, is used to provide a more secure and sophisticated encryption/decryption process. The first and second preferred embodiments relate to symmetric encryption/decryption systems and methods, and the third and fourth preferred embodiments relate to asymmetric encryption/decryption systems and methods.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other objects and advantages of the present invention will become apparent and more readily appreciated from the following detailed description of the presently preferred exemplary embodiment of the invention taken in conjunction with the accompanying drawings, of which:

Fig. 1A illustrates a conventional symmetric encryption/decryption system having a sender's computer system and a recipient's computer system;

Fig. 1B illustrates a flow chart of a conventional symmetric encryption/decryption method for encrypting/decrypting data using the system of Fig. 1A;

Fig. 2A illustrates a conventional asymmetric encryption/decryption system having a sender's computer system and a recipient's computer system;

Fig. 2B illustrates a flow chart of a conventional asymmetric encryption/decryption method for encrypting/decrypting data using the system of Fig. 2A;

Fig. 3A illustrates a system for providing brokered symmetric encryption/decryption in accordance with the first preferred embodiment of the present invention;

Fig. 3B illustrates a flow chart of a method for encrypting/decrypting data using the brokered symmetric system of Fig. 3A in accordance with the first preferred embodiment of the present invention;

Fig. 4A illustrates a system for providing brokered symmetric encryption/decryption in accordance with the second preferred embodiment of the present invention;

Fig. 4B illustrates a flow chart of a method for encrypting/decrypting data using the brokered symmetric system of Fig. 4A in accordance with the second preferred embodiment of the present invention;

Fig. 5A illustrates a system for providing brokered asymmetric encryption/decryption in accordance with the third preferred embodiment of the present invention;

Fig. 5B illustrates a flow chart of a method for encrypting/decrypting data using the brokered asymmetric system of Fig. 5A in accordance with the third preferred embodiment of the present invention;

Fig. 6A illustrates a system for providing brokered asymmetric encryption/decryption in accordance with the fourth preferred embodiment of the present invention; and

Fig. 6B illustrates a flow chart of a method for encrypting/decrypting data using the brokered asymmetric system of Fig. 6A in accordance with the fourth preferred embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention will now be described in greater detail, which will serve to further the understanding of the preferred embodiments of the present invention. As described elsewhere herein, various refinements and substitutions of the various embodiments are possible based on the principles and teachings herein.

The preferred embodiments of the present invention will be described with reference to Figs. 3 - 6, wherein like components and steps are designated by like reference numerals throughout the various figures. Further, specific parameters and steps are provided herein, and are intended to be explanatory rather than limiting.

The present invention is directed to systems and methods for symmetric and asymmetric encryption and decryption. The present invention provides methods for encrypting and decrypting sensitive and private data transmitted from a sender to a recipient over a distributed communication system such as the Internet. Although the Internet will be used as the preferred distributed communication system, other systems such as a private network (leased lines, X.25, Frame Relay, ISDN, ATM, etc.), Intranet, LAN, MAN, WAN, and the like may be used in accordance with the present invention.

The encryption/decryption processes of the present invention uses a broker agent (i.e., a server) to encrypt and decrypt data and/or session keys during the transmission of the data from the sender to the recipient. The encryption processes presented herein are believed to be more advanced than conventional processes because the recipient does not have access to the sender's private and public keys and vice

versa. A trusted third party, i.e., broker, is used to provide a more secure and sophisticated encryption/decryption processes. In this manner, the sender can send encrypted data to various recipients without needing access to the recipients' keys or certificates. In other words, unlike the conventional systems and methods where the sender and recipient need to exchange key or certificate information before sending data, the intermediate broker performs such role. As described in greater detail below, the first and second preferred embodiments relate to symmetric encryption/decryption systems and methods, and the third and fourth preferred embodiments relate to asymmetric encryption/decryption systems and methods.

The first and second preferred embodiments of the present invention relate to symmetric encryption/decryption systems and methods. Brokered symmetric encryption/decryption allows the sender to transmit the encrypted data to the recipient without either party having knowledge of the each other's security keys. This is accomplished by using the trusted third party, an intermediate or broker agent. The security keys can be private or public, and be passwords or Public Key Infrastructure (PKI) certificates. Other known keys and certificates may be used in accordance with this embodiment.

Fig. 3A illustrates a system for providing brokered symmetric encryption/decryption in accordance with the first preferred embodiment of the present invention. The sender uses a sender's computer system 310 to transmit data to a recipient's computer system 320 via the Internet 18. However, unlike the conventional systems, an intermediate party, a trusted broker 300, is used to provide a more sophisticated and secure encryption/decryption system and method.

As illustrated, the sender's system 310 includes and/or has access to a sender's security key 312, and a recipient's system 320 includes and/or has access to a recipient's security key 322. The broker's system/server 300 includes and/or has access to both the sender's security key 312 and the recipient's security key 322. In this system, the sender's system 310 does not have nor has access to any of the recipient's keys or broker's keys, and the recipient's system 320 does not have nor has access to any of the sender's keys or broker's keys.

In this and other embodiments of the present invention, the sender's system, recipient's system, and the broker's system/server can retrieve the various keys from other locations (i.e., server, database) on the Internet/WWW. Additionally, the sender's system and the recipient's system discussed throughout herein are preferably any computing device having Internet access capabilities such as a personal computer, server, laptop computer, digital cellular phone, PDA (portable digital assistant), webtv, and the like. Likewise, the broker's system is preferably a server, but may also be any computing device having Internet access capabilities as described above. The sender, recipient, and broker can access the Internet 18 via hardwire or wireless, using for example, a conventional modem, xDSL modem, cable modem, RF,

or other conventional methods known in the art.

Further, the encrypting and decrypting software programs that are stored in the computer systems (sender, recipient, and broker) described herein are preferably written in a language most suitable for encryption/decryption applications. Such language includes C, C++, Java, Perl, but others languages than those stated above may be used in the present invention.

Although only one sender, one recipient and one broker are illustrated throughout the figures, it is understood that the other preferred embodiments of the present invention can utilize any number of senders, recipients, and brokers, and other similar parties may be substituted for the ones described above. Moreover, one skilled in the art will appreciate that various substitutions and modifications can be made to the examples described herein while remaining within the spirit and scope of the present invention.

In order to implement the present invention between the sender, recipient, and broker, one or more parties must be capable of generating, retrieving, and/or locally storing the various keys on their respective systems. For example, the sender's system 310 should be capable of generating, retrieving, and/or storing the sender's security key 312. Likewise, the recipient's system 320 should be capable of generating, retrieving, and/or storing the recipient's security key 322. In addition, the broker's system 300 should be capable of generating, retrieving, and/or storing the sender's security key 312 and the recipient's security key 322.

Fig. 3B illustrates a flow chart of a method for encrypting/decrypting data using the brokered symmetric system of Fig. 3A in accordance with the first preferred embodiment of the present invention. Reference will be made concurrently to Figs. 3A and 3B for a more complete understanding of this method. During operation in accordance with the first preferred embodiment, the sender's system 310 encrypts the data using the sender's security key 312 in step 400. Thereafter, the sender transmits the encrypted data to the broker's system 300 via the Internet 18 in step 402. Steps 400-402 are performed at the sender's system 310.

Next, in step 404, the broker receives the encrypted data from the sender. The broker's system 300 then searches for and locates the sender's security key 312 from its database (or other locations on the Internet/WWW) in step 406 so that the data can be decrypted in step 408. The broker's system 300 again searches the database (or other locations on the Internet/WWW) to locate the recipient's security key 322 in step 410. The data is re-encrypted using the recipient's security key 332 in step 412. The re-encrypted data is then transmitted to the recipient's system 320 via the Internet 18 in step 414. Steps 404-414 are performed at the broker's system 300.

In step 416, the recipient receives the encrypted data from the broker. The recipient's system 320

next decrypts the data using the recipient's security key 322 so that the data can be turned back to its original form in step 418. After the data is decrypted, the recipient views and uses the data in step 420. Steps 416-220 are performed at the recipient's system 320.

The symmetric encryption/decryption system and method described above provides a secure manner of transmitting data from the sender to the recipient. However, the first preferred embodiment can be improved slightly by providing an even more secure symmetric encryption/decryption. In the first preferred embodiment, the data is in a decrypted state for a very short period of time at the broker's system 300. The data is in the decrypted state during steps 408-410 when the data is decrypted with the sender's security key 312 and then re-encrypted with the recipient's security key 322. As a result, the data may be vulnerable from unauthorized users during this short period of time.

Accordingly, the second preferred embodiment of the present invention provides an even more secure symmetric encryption/decryption system and method. Fig. 4A illustrates a system for providing brokered symmetric encryption/decryption in accordance with the second preferred embodiment of the present invention. As described earlier herein, the sender uses a sender's computer system 510 to transmit data to a recipient's computer system 520 via the Internet 18. An intermediate party, a trusted broker 500, is used to provide a more sophisticated and secure encryption/decryption system and method.

As illustrated, the sender's system 510 includes and/or has access to a generated session key 530 and a sender's security key 512. Likewise, the recipient's system 520 includes and/or has access to the generated session key 530 and a recipient's security key 522. The broker's system/server 500 includes and/or has access to both the sender's security key 512 and the recipient's security key 522. In this system, the sender's system 510 does not have nor has access to any of the recipient's keys or broker's keys, and the recipient's system 520 does not have nor has access to any of the sender's keys or broker's keys.

In the context of this disclosure, the generated session key is a key associated with a unique value, data, etc. that is specific to the document/message. For example, in an online stock trade context, the generated session key can be associated with the exact date and time that the trade was conducted. Thus, each session key is unique for each particular document/message.

Fig. 4B illustrates a flow chart of a method for encrypting/decrypting data using the brokered symmetric system of Fig. 4A in accordance with the second preferred embodiment of the present invention. Reference will be made concurrently to Figs. 4A and 4B for a more complete understanding of this method.

During operation in accordance with the second preferred embodiment, the sender's system 510 generates and/or retrieves the session key 530 in step 600. The session key 530 is preferably generated

using a cryptographic random key generator, as known in the art. In the alternative, a seed containing data specific to the document/message can be used for generating the session key 530 using a security algorithm, such as RSA's MD5Random Algorithm. While the RSA MD5Random Algorithm is preferred, other security algorithms may be used in the present invention to generate the session key 530. Thus, the generated session key 530 can be a random number having at least 128-bits in length.

After generating and/or retrieving the session key 530, it is used to encrypt the data at the sender's system 510 in step 602. Thereafter, the generated session key 530 is encrypted using the sender's security key 512 residing on or retrieved from the sender's system 510 in step 604. In step 606, the sender transmits both the encrypted session key 530 and data to the broker's system 500 via the Internet 18. Steps 600-606 are performed at the sender's system 510.

Next, in step 608, the broker receives the encrypted session key 530 and data from the sender. The broker's system 500 then searches for and locates the sender's security key 512 from its database (or other locations on the Internet/WWW) in step 610 and decrypts the session key 530 using the sender's security key 512 in step 612. After decrypting the session key 530, the broker's system 500 searches for and locates the recipient's security key 522 from its database (or other locations on the Internet/WWW) in step 614 so that the session key 530 can be re-encrypted using the recipient's security key 522 in step 616. The re-encrypted session key 530 and the data are then transmitted to the recipient's system 520 via the Internet 18 in step 618. Steps 608-618 are performed at the broker's system 500.

In step 620, the recipient receives the re-encrypted session key 530 and data from the broker. The recipient's system 520 next decrypts the re-encrypted session key 530 using the recipient's security key 522 residing or retrieved from therein in step 622 since the session key 530 was re-encrypted by the broker's system 500 using the recipient's security key in step 616. After the session key 530 is decrypted, it is used to decrypt the data in step 624 so that the data can be turned back to its original form. Thereafter, the recipient views and uses the data in step 626. Steps 620-626 are performed at the recipient's system 520.

An important aspect of the second embodiment described above is that data remains encrypted as it is transmitted from the sender's system 510 to the recipient's system 520. It is again worthwhile to note that the broker's system 500 does not decrypt the data, but decrypts and encrypts the generated session key 530 using the sender's security key 512 and recipient's security key 522, respectively. The broker again must be a trusted agent of both the sender and the recipient since it has the ability to decrypt the data after decrypting the generated session key 530 in step 612.

Fig. 5A illustrates a system for providing brokered asymmetric encryption/decryption in accordance with the third preferred embodiment of the present invention. Brokered asymmetric

encryption/decryption allows the sender to transmit encrypted data to the recipient without knowledge of the recipient's public key. This is accomplished by allowing the trusted third party, broker, to know the public keys of both the sender and the recipient. The public key is preferably a PKI certificate, but other known keys and certificates may be used in accordance with the present invention.

In Fig. 5A, the sender uses a sender's computer system 60 to transmit data to a recipient's computer system 70 via the Internet 18. However, unlike the conventional systems, an intermediate party, a broker 50, is used to provide a more sophisticated and secure encryption/decryption system. As illustrated, the sender's system 110 includes and/or has access to a broker's public key 62 and a sender's private key 64. Likewise, a recipient's computer system 70 includes and/or has access to the broker's public key 62 and a recipient's private key 74. In addition, the broker's system/server 50 includes and/or has access to a broker's private key 52, a sender's public key 54, and a recipient's public key 56. In this system, the sender's system 60 does not have nor has access to the recipient's public key 56, and the recipient's system 70 does not have nor has access to the sender's public key 54.

Again, to implement the present invention between the sender, recipient, and broker using the asymmetric brokered methods and systems, one or more parties must be capable of generating, retrieving, and/or locally storing the various keys on their respective systems. For example, the sender's system 60 should be capable of generating, retrieving, and/or storing the broker's public key 62 and the sender's private key 64. Likewise, the recipient's system 70 should be capable of generating, retrieving, and/or storing the broker's public key 62 and the recipient's private key 74. In addition, the broker's system 100 should be capable of generating, retrieving, and/or storing the broker's private key 52, sender's public key 54, and recipient's public key 56.

Fig. 5B illustrates a flow chart of a method for encrypting/decrypting data using the brokered asymmetric system of Fig. 5A in accordance with the third preferred embodiment of the present invention. Reference will be made concurrently to Figs. 5A and 5B for a more complete understanding of this method. During operation in accordance with the third preferred embodiment, the sender's system 60 encrypts the data using the broker's public key 62 in step 80. In step 82, the sender transmits the encrypted data to the broker's system 50 via the Internet 18. Steps 80-82 are performed at the sender's system 60.

Next, in step 84, the broker's system 50 receives encrypted data from the sender's system 60. The broker's system 50 then searches for and locates the broker's private key 52 in order to decrypt the data in step 86. After decrypting the data, the broker's system 50 searches for and locates the recipient's public key 56 from its database (or other locations on the Internet/WWW) in step 88 so that the data can be re-encrypted using the recipient's public key 56 in step 90. The re-encrypted data is then transmitted

to the recipient's system 70 via the Internet 18 in step 92. Steps 84-92 are performed at the broker's system 50.

In step 94, the recipient's system 70 receives the re-encrypted data from the broker's system 50. The recipient's system 70 next decrypts the data using the recipient's private key 74 residing or retrieved from therein since the data was re-encrypted by the broker's system 50 using the recipient's public key 56 in step 90. After the data is turned back to its original form, the recipient views and uses the data in step 98. Steps 94-98 are performed at the recipient's system 70.

Fig. 6A illustrates a system for providing brokered asymmetric encryption/decryption in accordance with the fourth preferred embodiment of the present invention. In Fig. 6A, the sender uses a sender's computer system 110 to transmit data to a recipient's computer system 120 via the Internet 18. As illustrated, the sender's system 110 includes and/or has access to a broker's public key 112, a generated session key 114, and a sender's private key 116. Likewise, a recipient's computer system 120 includes and/or has access to the generated session key 114 and a recipient's private key 122. The recipient's system 120 will also require the broker's public key 112 if the recipient desires to transmit data to the sender's system 110 using the present asymmetric method. In addition, the broker's system/server 100 includes and/or has access to a broker's private key 102, a sender's public key 104, and a recipient's public key 106. Again, in this system, the sender's system 110 does not have nor has access to the recipient's public key 106, and the recipient's system 120 does not have nor has access to the sender's public key 104.

Again, to implement the present invention between the sender, recipient, and broker, one or more parties must be capable of generating, retrieving, and/or locally storing the various keys on their respective systems. For example, the sender's system 110 should be capable of generating, retrieving, and/or storing the session key 114, the broker's public key 112, and the sender's private key 116. Likewise, the recipient's system 120 should be capable of generating, retrieving, and/or storing the broker's public key 112, the recipient's private key 122, and the session key 114 (in the case when recipient desires to send data to the sender). In addition, the broker's system 100 should be capable of generating, retrieving, and/or storing the broker's private key 102, sender's public key 104, and the recipient's public key 106.

Fig. 6B illustrates a flow chart of a method for encrypting/decrypting data using the brokered asymmetric system of Fig. 6A in accordance with the fourth preferred embodiment of the present invention. Reference will be made concurrently to Figs. 6A and 6B for a more complete understanding of this method. During operation in accordance with the fourth preferred embodiment, the sender's system 110 generates and/or retrieves the session key 114 in step 200 in a manner similar to that

described earlier herein (i.e., using a cryptographic random key generator).

After generating the session key 114, it is used to encrypt the data at the sender's system 110 in step 202. Thereafter, the generated session key 114 is encrypted using the broker's public key 112 residing on or retrieved from the sender's system 110 in step 204. In step 206, the sender's system 110 transmits both the encrypted data and the session key 114 to the broker's system 100 via the Internet 18 in step 206. Steps 200-206 are performed at the sender's system 110.

Next, in step 208, the broker's system 100 receives the encrypted session key 114 and data from the sender's system 110. The broker's system 100 then decrypts the session key 114 using the broker's private key 102 in step 210. After decrypting the session key 114, the broker's system 100 searches for and locates the recipient's public key 106 from its database (or other locations on the Internet/WWW) in step 212 so that the session key 114 can be re-encrypted using the recipient's public key 106 in step 214. The re-encrypted session key 114 and the data are then transmitted to the recipient's system 120 via the Internet 18 in step 216. Steps 208-216 are performed at the broker's system 100.

In step 218, the recipient's system 120 receives the re-encrypted session key 114 and data from the broker's system 100. The recipient's system 120 next decrypts the session key 114 using the recipient's private key 122 residing or retrieved from therein since the session key 114 was re-encrypted by the broker's system 100 using the recipient's public key 106 in step 214. After the session key 114 is decrypted, it is used to decrypt the data in step 222 so that the data can be turned back to its original form. Thereafter, the recipient views and uses the data in step 224. Steps 218-224 are performed at the recipient's system 120.

An important aspect of the asymmetric encryption/decryption system and method described above is that data remains encrypted as it is transmitted from the sender's system 110 to the recipient's system 120. It is worthwhile to note that the broker's system 100 does not decrypt the data, but decrypts and encrypts the session key 114 using the broker's private key 102 and recipient's public key 106, respectively. Thus, the broker must be a trusted agent of both the sender and the recipient since it has the ability to decrypt the data after decrypting the session key 114 in step 210. In other words, the decrypted session key 114 can be used to decrypt the data at the broker's system 100.

In an alternative embodiment of the asymmetric encryption/decryption system and method described above, digital signing and verification can also be implemented. In this manner, the recipient's system 120 will include the sender's public key. The sender transmits the data from the sender's system 110 with a signed signature from the sender's private key 116 to the recipient's system 120. The sender's signature is transmitted unaltered and unchanged to the recipient's system 120 via the Internet 18 and broker's system 100. The recipient can then decrypt the signature using the sender's public key

contained therein, thereby verifying that the data originated from the sender's system 110, and not from a different unknown sender.

As discussed above, in certain embodiments of the present invention, the data is encrypted and decrypted once while the corresponding session key is encrypted and decrypted twice during the entire process. Accordingly, these added security measures provide assurance that the data in the documents, email, etc., is secure and confidential as it travels from the sender to the recipient. Because the present invention uses the trusted broker for encryption and decryption, the present systems and methods are more advanced than conventional encryption/decryption systems and methods.

In the previous descriptions, numerous specific details are set forth, such as specific algorithms, encryption/decryption process, distribution channel, etc., to provide a thorough understanding of the present invention. However, as one having ordinary skill in the art would recognize, the present invention can be practiced without resorting to the details specifically set forth. For example, other secure algorithms may be substituted for the MD5Random Algorithm.

Although various preferred embodiments of the present invention have been disclosed for illustrative purposes, those skilled in the art will appreciate that various modifications, additions and/or substitutions are possible without departing from the scope and spirit of the present invention as disclosed in the claims.

We claim:

1. A system for transmitting data on a distributed communication channel, comprising:

a sender system having a sender key for encrypting the data;

an intermediate system for receiving the data encrypted with the sender key from the sending system, wherein the intermediate system includes a means for allowing the data to be decrypted by a recipient key; and

a recipient system having the recipient key for decrypting the data received from the intermediate system.

2. A system according to claim 1, wherein the distributed communication channel comprises the Internet.

3. A system according to claim 1, wherein the means for allowing the data to be decrypted by the recipient key comprises decrypting the data using the sender key and re-encrypting the data using the recipient key.

4. A system according to claim 3, wherein the intermediate system has access to the sender key and the recipient key.

5. A system according to claim 1, wherein each of the sender key and the recipient key comprises one of a public key, private key, password, and certificate.

6. A system according to claim 1, wherein each of the sender system, the recipient system, and the intermediate system comprises one of a computer, server, digital cellular phone, and portable digital assistant.

7. A method of transmitting electronic data by a sender system to a recipient system via a distributed communication system, the method comprising:

(1) encrypting data using a sender key at the sender system;

(2) transmitting the encrypted data from the sender system to an intermediate system via the distributed communication system;

(3) decrypting the data using the sender key at the intermediate system;

(4) re-encrypting the data using a recipient key at the intermediate system;

(5) transmitting the re-encrypted data from the intermediate system to the recipient system via the distributed communication system; and

(6) decrypting the re-encrypted data using the recipient key at the recipient system.

8. A method according to claim 7, wherein the distributed communication channel comprises the Internet.

9. A method according to claim 7, wherein the intermediate system has access to the sender key and

the recipient key.

10. A method according to claim 7, wherein each of the sender key and the recipient key comprises one of a public key, private key, password, and certificate.

11. A method according to claim 7, wherein each of the sender system, the recipient system, and the intermediate system comprises one of a computer, server, digital cellular phone, and portable digital assistant.

12. A system for transmitting data on a distributed communication channel, comprising:

a sender system having a sender key for encrypting a session key, wherein the session key is used for encrypting the data;

an intermediate system for receiving the session key and the data from the sending system, wherein the intermediate system includes a means for allowing the session key to be decrypted by a recipient key; and

a recipient system having the recipient key for decrypting the session key received from the intermediate system, wherein the session key is used for decrypting the data.

13. A system according to claim 12, wherein the distributed communication channel comprises the Internet.

14. A system according to claim 12, wherein the means for allowing the session key to be decrypted by the recipient key comprises decrypting the session key using the sender key and re-encrypting the session key using the recipient key.

15. A system according to claim 14, wherein the intermediate system has access to the sender key and the recipient key.

16. A system according to claim 12, wherein each of the sender key and the recipient key comprises one of a public key, private key, password, and certificate.

17. A system according to claim 12, wherein each of the sender system, the recipient system, and the intermediate system comprises one of a computer, server, digital cellular phone, and portable digital assistant.

18. A system according to claim 12, wherein the session key includes a unique value.

19. A system according to claim 12, wherein the session key is generated using a random key generator.

20. A system according to claim 12, wherein the session key includes at least 128 bits in lengths.

21. A method of transmitting electronic data by a sender system to a recipient system via a distributed communication system, the method comprising:

(1) encrypting data using a session key at the sender system;

(2) encrypting the session key using a sender key at the sender system;

(3) transmitting the encrypted session key and data from the sender system to an intermediate system via the distributed communication system;

(4) receiving the encrypted session key and data at the intermediate system;

(5) decrypting the session key using the sender key at the intermediate system;

(6) re-encrypting the session key using a recipient key at the intermediate system;

(7) transmitting the re-encrypted session key and encrypted data from the intermediate system to the recipient system via the distributed communication system;

(8) decrypting the re-encrypted session key using the recipient key at the recipient system; and

(9) decrypting the encrypted data using the session key at the recipient system.

22. A method according to claim 21, wherein the distributed communication channel comprises the Internet.

23. A method according to claim 21, wherein the intermediate system has access to the sender key and the recipient key.

24. A method according to claim 21, wherein each of the sender key and the recipient key comprises one of a public key, private key, password, and certificate.

25. A method according to claim 21, wherein each of the sender system, the recipient system, and the intermediate system comprises one of a computer, server, digital cellular phone, and portable digital assistant.

26. A method according to claim 21 further comprising generating the session key at the sender system.

27. A method according to claim 26, wherein the session key includes a unique value.

28. A method according to claim 26 further comprising generating the session key using a random key generator.

29. A method according to claim 26, wherein the session key includes at least 128 bits in lengths.

30. A system for transmitting data on a distributed communication channel, comprising:

a sender system having an intermediate key for encrypting a session key, wherein the session key is used for encrypting the data;

an intermediate system for receiving the session key and the data from the sending system, wherein the intermediate system includes a means for allowing the session key to be decrypted by a recipient key; and

a recipient system having the recipient key for decrypting the session key received from the intermediate system, wherein the session key is used for decrypting the data.

31. A system according to claim 30, wherein the distributed communication channel comprises the Internet.

32. A system according to claim 30, wherein the means for allowing the session key to be decrypted by the recipient key comprises decrypting the session key using the intermediate key and re-encrypting the session key using the recipient key.

33. A system according to claim 32, wherein the intermediate system has access to the sender key, the recipient key, and the intermediate key.

34. A system according to claim 30, wherein each of the sender key, the recipient key, and the intermediate key comprises one of a public key, private key, password, and certificate.

35. A system according to claim 30, wherein each of the sender system, the recipient system, and the intermediate system comprises one of a computer, server, digital cellular phone, and portable digital assistant.

36. A system according to claim 30, wherein the session key includes a unique value.

37. A system according to claim 30, wherein the session key is generated using a random key generator.

38. A system according to claim 30, wherein the session key includes at least 128 bits in lengths.

39. A method of transmitting electronic data by a sender system to a recipient system via a distributed communication system, the method comprising:

(1) encrypting data using a session key at the sender system;

(2) encrypting the session key using an intermediate key at the sender system;

(3) transmitting the encrypted session key and data from the sender system to an intermediate system via the distributed communication system;

(4) receiving the encrypted session key and data at the intermediate system;

(5) decrypting the session key using the intermediate key at the intermediate system;

(6) re-encrypting the session key using a recipient key at the intermediate system;

(7) transmitting the re-encrypted session key and encrypted data from the intermediate system to the recipient system via the distributed communication system;

(8) decrypting the re-encrypted session key using the recipient key at the recipient system; and

(9) decrypting the encrypted data using the session key at the recipient system.

40. A method according to claim 39, wherein the distributed communication channel comprises the Internet.

41. A method according to claim 39, wherein the intermediate system has access to the sender key, the recipient key, and the intermediate key.

42. A method according to claim 39, wherein each of the sender key, the recipient key, and the intermediate key comprises one of a public key, private key, password, and certificate.

43. A method according to claim 39, wherein each of the sender system, the recipient system, and the intermediate system comprises one of a computer, server, digital cellular phone, and portable digital assistant.

44. A method according to claim 39 further comprising generating the session key at the sender system.

45. A method according to claim 44, wherein the session key includes a unique value.

46. A method according to claim 44 further comprising generating the session key using a random key generator.

47. A method according to claim 46, wherein the session key includes at least 128 bits in lengths.

48. A method of encrypting and decrypting data sent from a sender system to a recipient system through an intermediate system, wherein neither the sender system and the recipient system have knowledge of the others' security keys, the method comprising:

encrypting the data using a first key residing on the sender system;

transmitting the encrypted data from the sending device to the intermediate system, where the intermediate system provides a means for decrypting the data using a second key on a recipient system;

transmitting the encrypted data from the intermediate device to the recipient system; and

decrypting the data using the second key on the recipient device.

49. A method according to claim 48, wherein the means for allowing the data to be decrypted by the second key comprises decrypting the data using the first key and re-encrypting the data using the second key at the intermediate system.

50. A method according to claim 48 further comprising generating a session key at the sender system.

51. A method according to claim 50, wherein the session key includes a unique value.

52. A method according to claim 50 further comprising generating the session key using a random key generator.

53. A method according to claim 50, wherein the session key includes at least 128 bits in lengths.

54. A method according to claim 50 further comprising encrypting the session key using the first key such that the encrypted session key is used to encrypted the data on the sender system.

55. A method according to claim 54, wherein the means for allowing the data to be decrypted by the second key comprises decrypting the session key using the first key and re-encrypting the session key

using the second key at the intermediate system.

56. A method according to claim 55 further comprising decrypting the session key using the second key such that the decrypted session key is used to decrypt the data on the recipient system.

57. A method according to claim 48, wherein each of the first key and the second key comprises one of a public key, private key, password, and certificate.

58. A method according to claim 48, wherein each of the sender system, the recipient system, and the intermediate system comprises one of a computer, server, digital cellular phone, and portable digital assistant.

59. A system for transmitting data on a distributed communication channel, comprising:

a sender system having an intermediate key for encrypting the data;

an intermediate system for receiving the encrypted data from the sending system, wherein the intermediate system includes a means for allowing the data to be decrypted by a recipient key; and

a recipient system having the recipient key for decrypting the data received from the intermediate system.

60. A system according to claim 59, wherein the distributed communication channel comprises the Internet.

61. A system according to claim 59, wherein the means for allowing the data to be decrypted by the recipient key comprises decrypting the data using the intermediate key and re-encrypting the data using the recipient key.

62. A system according to claim 61, wherein the intermediate system has access to the recipient key and the intermediate key.

63. A system according to claim 59, wherein each of the sender key, the recipient key, and the intermediate key comprises one of a public key, private key, password, and certificate.

64. A system according to claim 59, wherein each of the sender system, the recipient system, and the intermediate system comprises one of a computer, server, digital cellular phone, and portable digital assistant.

65. A method of transmitting electronic data by a sender system to a recipient system via a distributed communication system, the method comprising:

(1) encrypting data using an intermediate key at the sender system;

(2) transmitting the encrypted data from the sender system to an intermediate system via the distributed communication system;

(3) decrypting the data using the intermediate key at the intermediate system;

(4) re-encrypting the data using a recipient key at the intermediate system;

(5) transmitting the re-encrypted data from the intermediate system to the recipient system via the distributed communication system; and

(6) decrypting the re-encrypted data using the recipient key at the recipient system.

66. A method according to claim 65, wherein the distributed communication channel comprises the Internet.

67. A method according to claim 65, wherein the intermediate system has access to the recipient key and the intermediate key.

68. A method according to claim 65, wherein each of the sender key, the recipient key, and the intermediate key comprises one of a public key, private key, password, and certificate.

69. A method according to claim 65, wherein each of the sender system, the recipient system, and the intermediate system comprises one of a computer, server, digital cellular phone, and portable digital assistant.

70. A method according to claim 65 further comprising generating the session key at the sender system.

71. A method according to claim 70, wherein the session key includes a unique value.

72. A method according to claim 70 further comprising generating the session key using a random key generator.

73. A method according to claim 70, wherein the session key includes at least 128 bits in lengths.

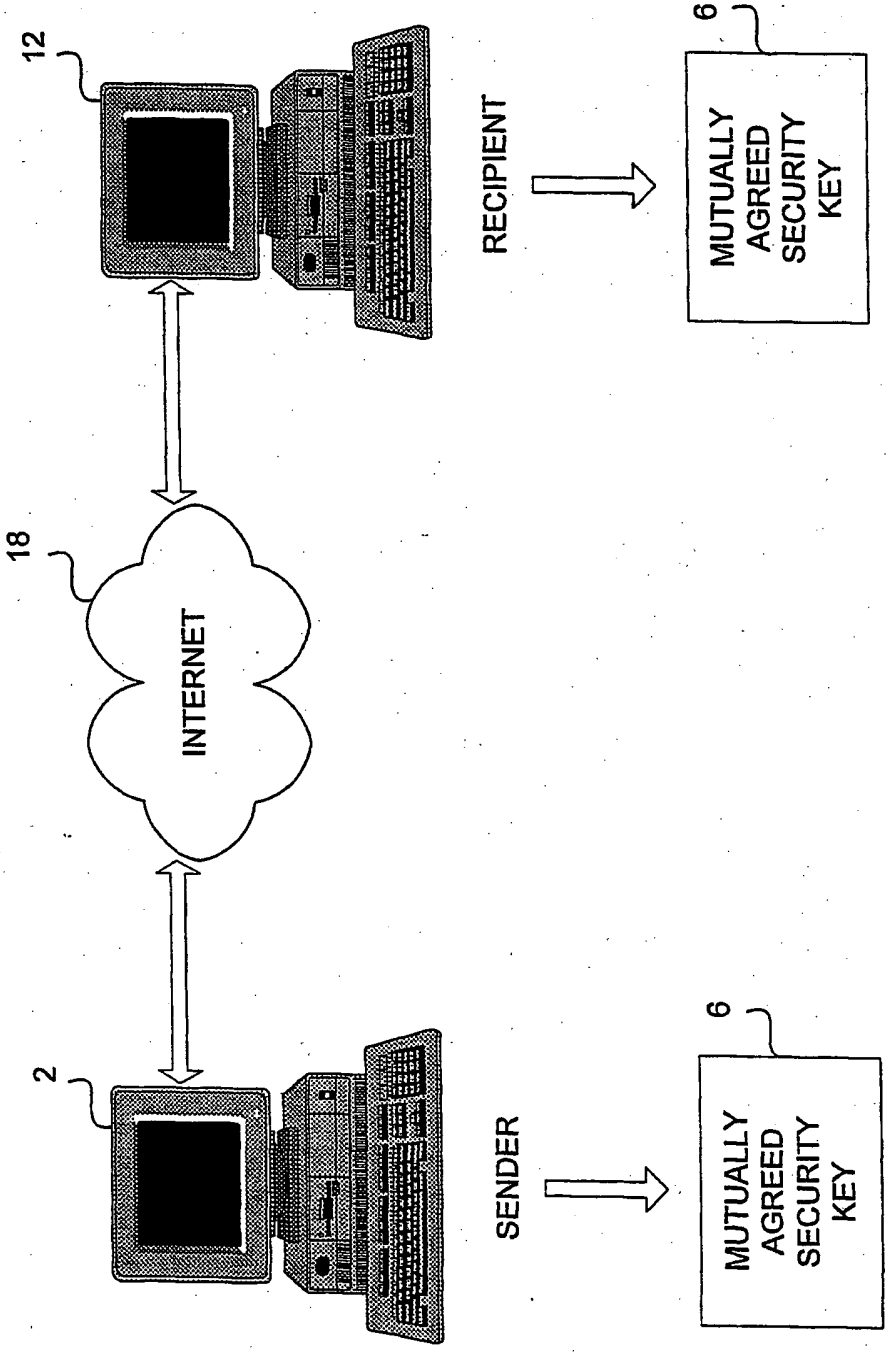

FIG. 1A (PRIOR ART - SYMMETRIC)

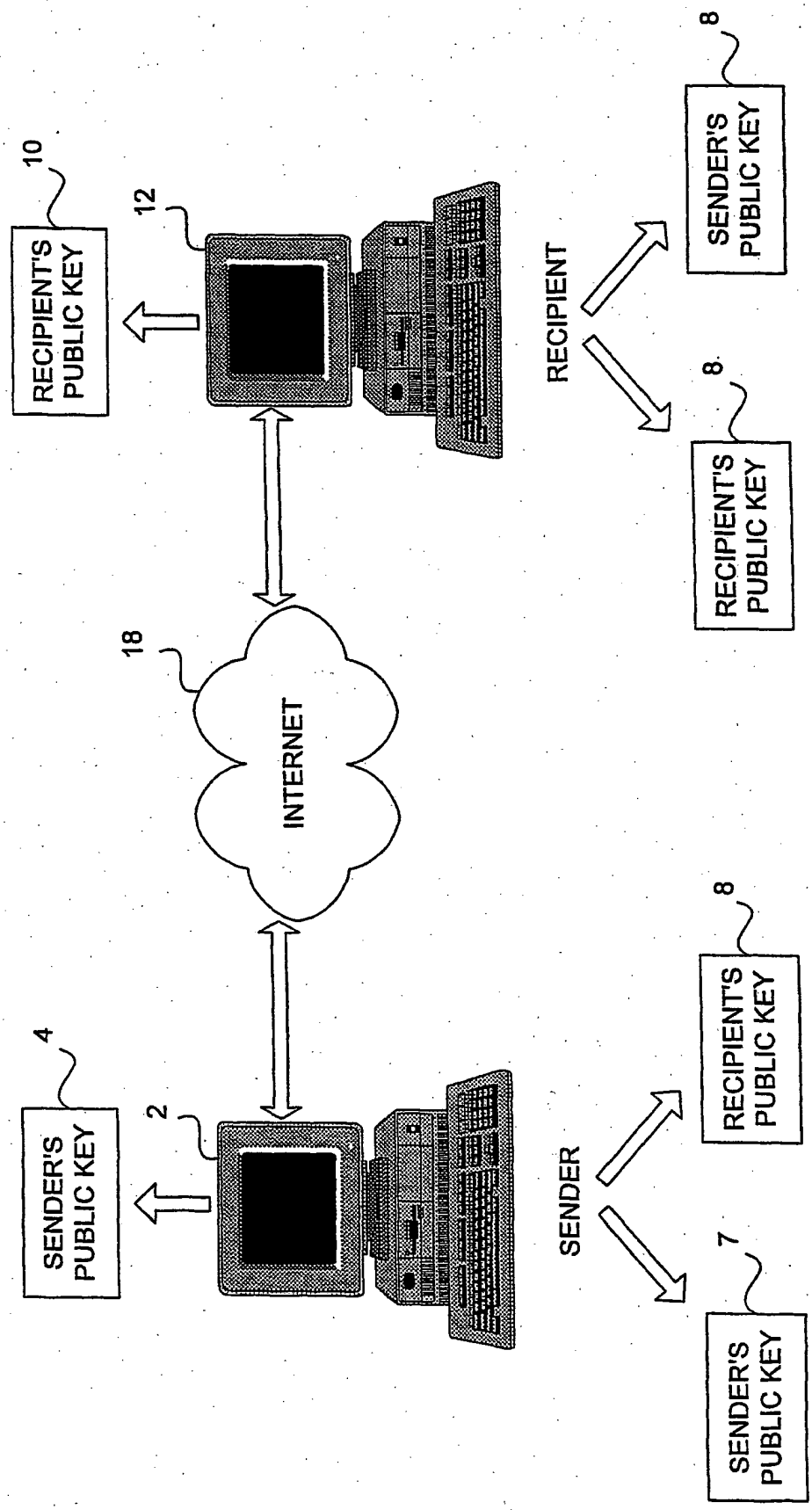

FIG. 2A (PRIOR ART - ASYMMETRIC)

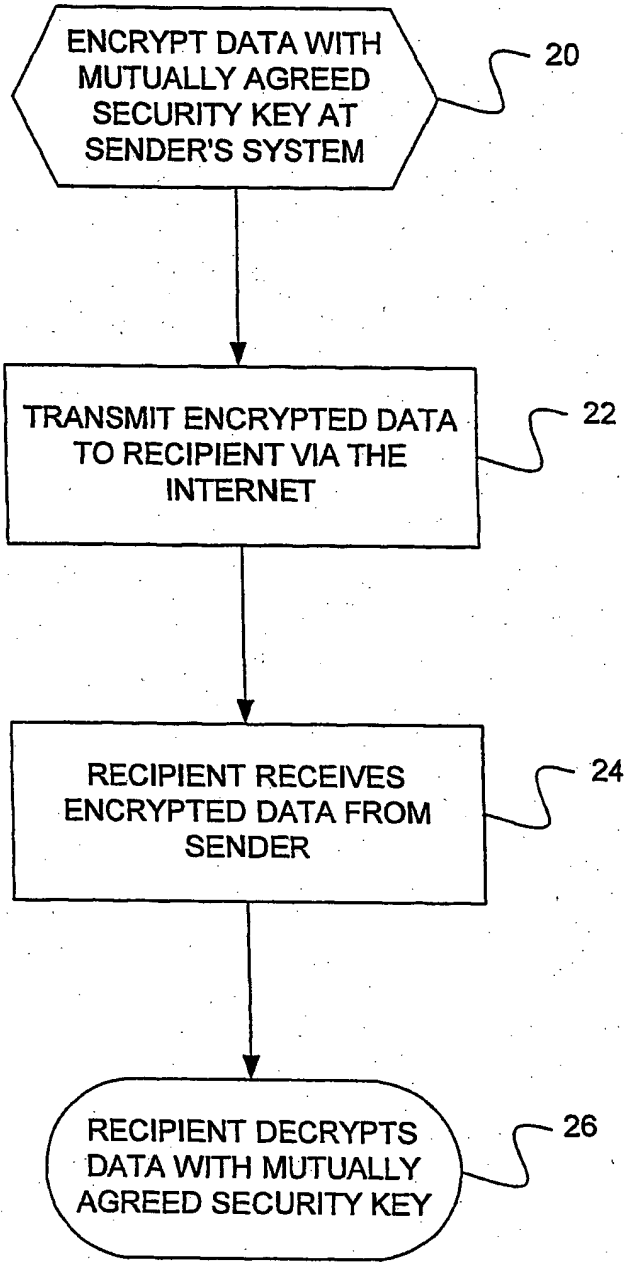

FIG. 1B (PRIOR ART - SYMMETRIC)

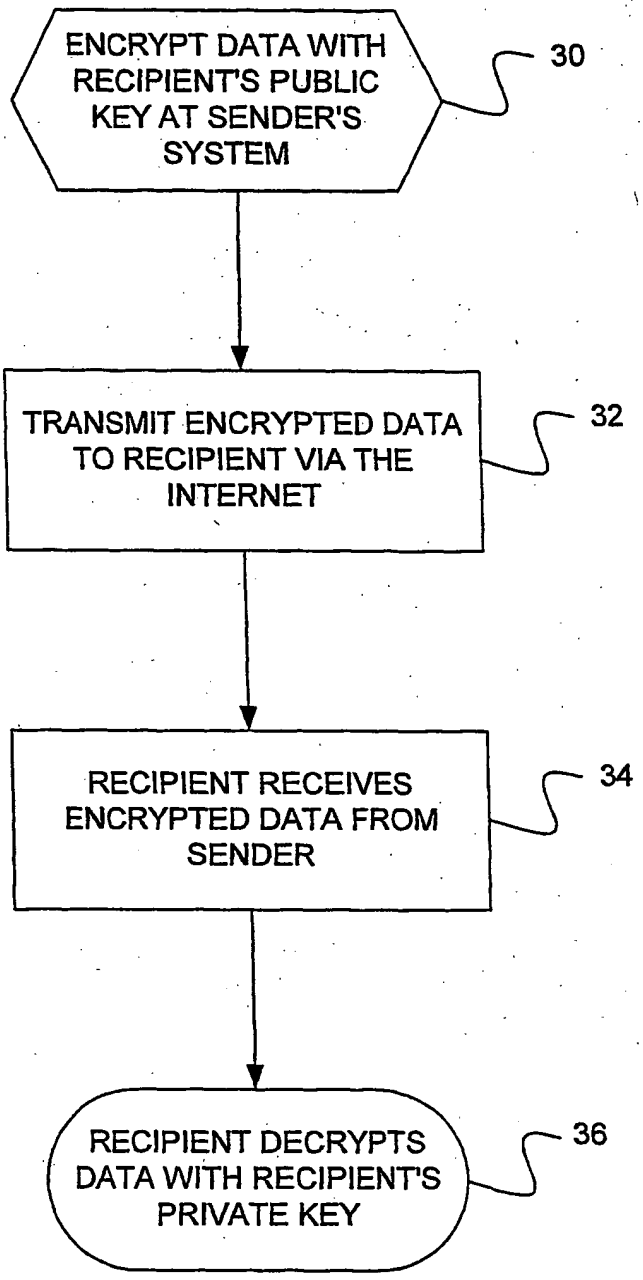

FIG. 2B (PRIOR ART - ASYMMETRIC)

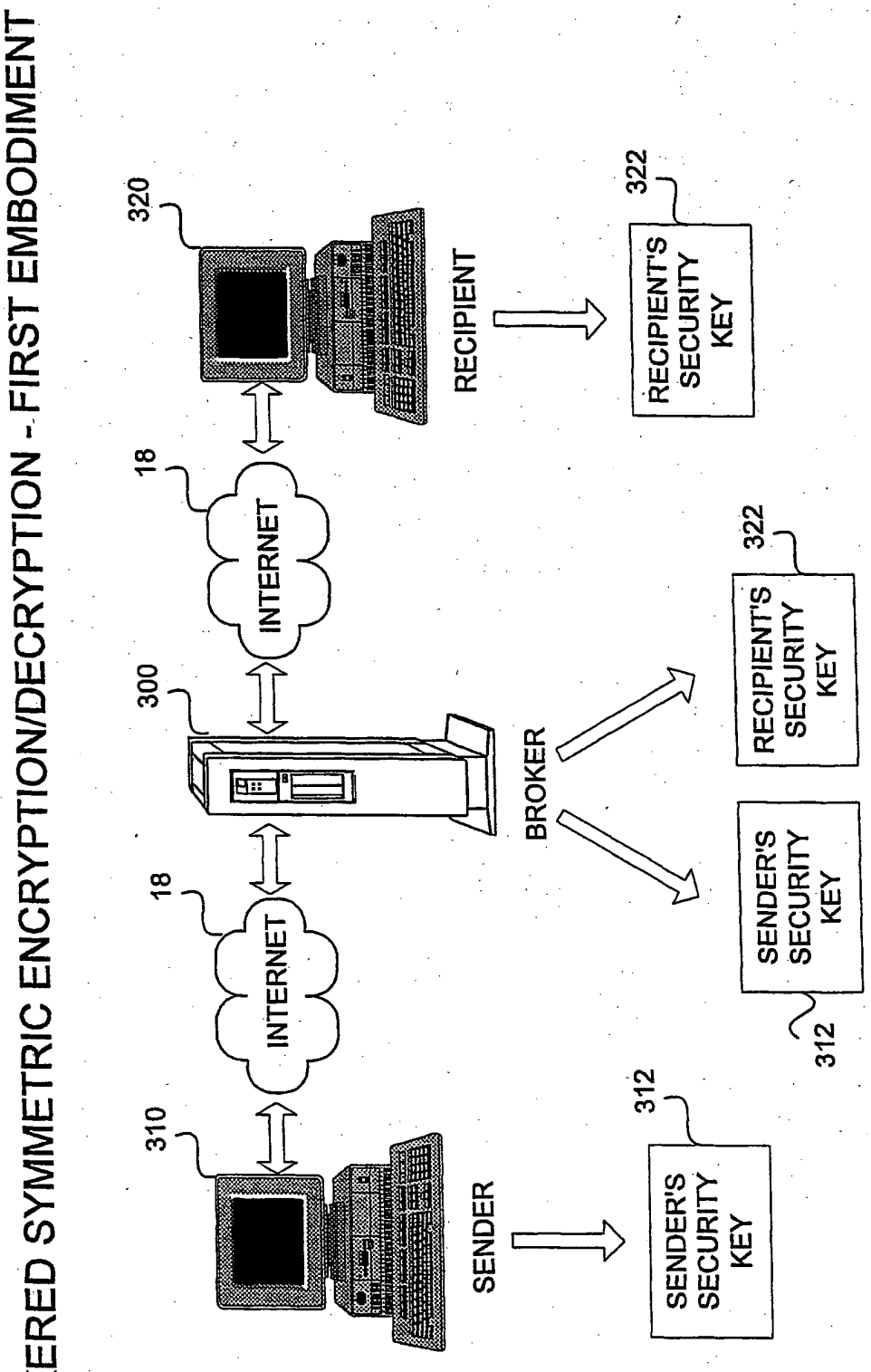
BROKERED SYMMETRIC ENCRYPTION/DECRYPTION - FIRST EMBODIMENT
320
RECIPIENT
322
RECIPIENT'S SECURITY KEY
18
INTERNET
300
BROKER
322
RECIPIENT'S SECURITY KEY
18
INTERNET
SENDER'S SECURITY KEY
312
310
SENDER
312
SENDER'S SECURITY KEY

FIG. 3A

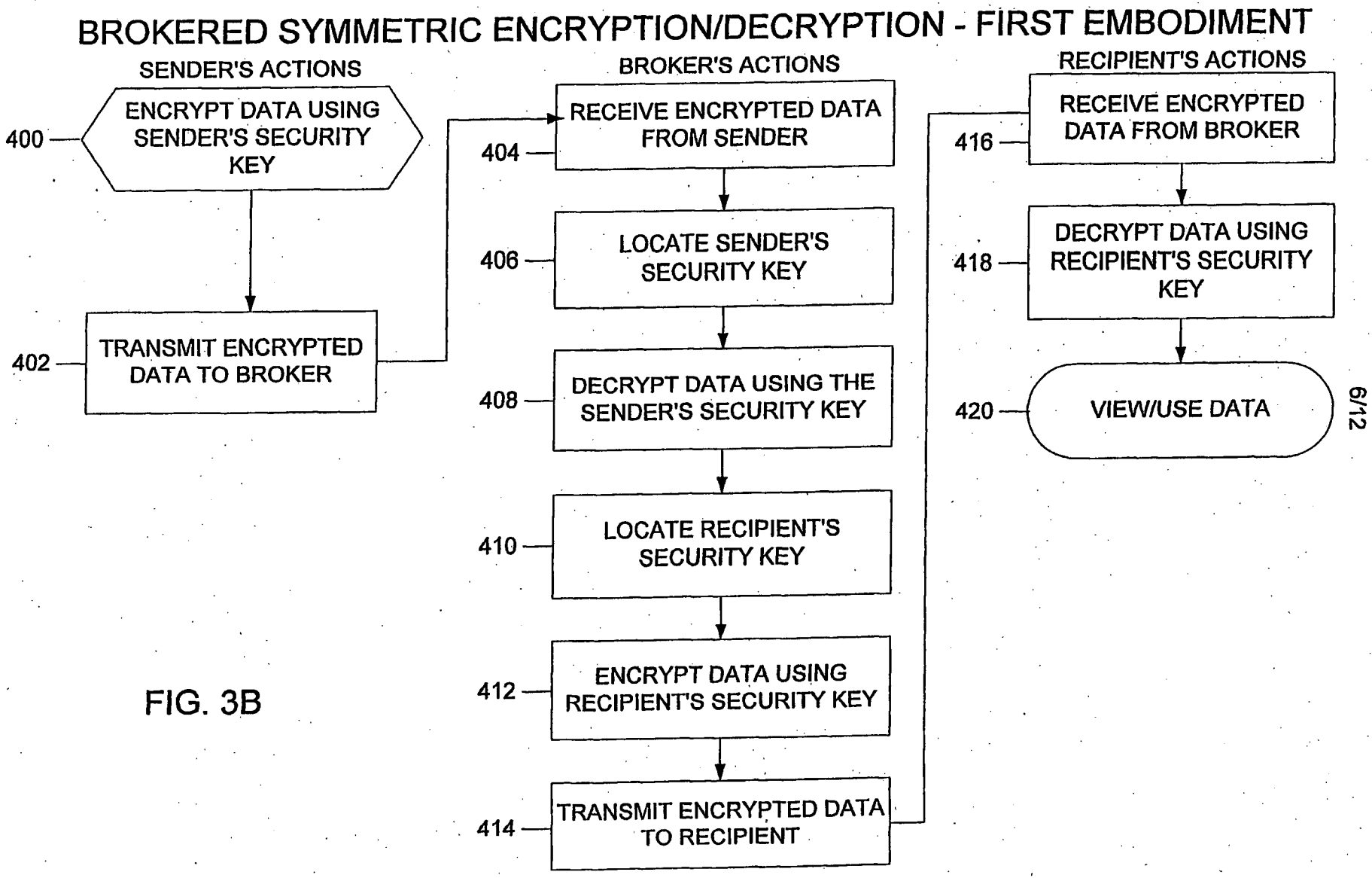
BROKERED SYMMETRIC ENCRYPTION/DECRYPTION - FIRST EMBODIMENT
SENDER'S ACTIONS
BROKER'S ACTIONS
RECIPIENT'S ACTIONS
400
ENCRYPT DATA USING SENDER'S SECURITY KEY
402
TRANSMIT ENCRYPTED DATA TO BROKER
404
RECEIVE ENCRYPTED DATA FROM SENDER
406
LOCATE SENDER'S SECURITY KEY
408
DECRYPT DATA USING THE SENDER'S SECURITY KEY
410
LOCATE RECIPIENT'S SECURITY KEY
412
ENCRYPT DATA USING RECIPIENT'S SECURITY KEY
414
TRANSMIT ENCRYPTED DATA TO RECIPIENT
416
RECEIVE ENCRYPTED DATA FROM BROKER
418
DECRYPT DATA USING RECIPIENT'S SECURITY KEY
420
VIEW/USE DATA

FIG. 3B

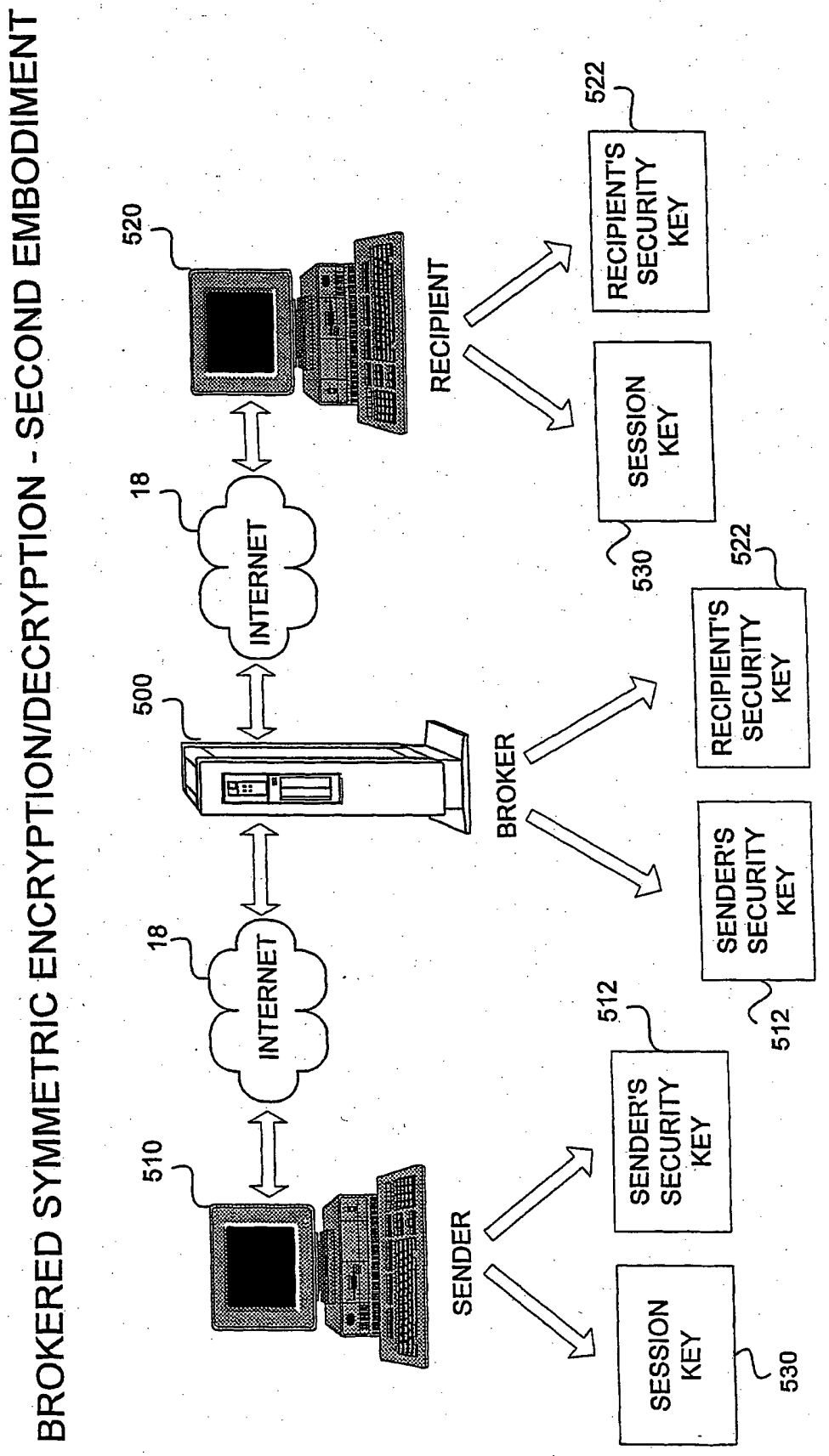
BROKERED SYMMETRIC ENCRYPTION/DECRYPTION - SECOND EMBODIMENT
520
RECIPIENT
522
RECIPIENT'S SECURITY KEY
SESSION KEY
530
18
INTERNET
500
BROKER
522
RECIPIENT'S SECURITY KEY
SENDER'S SECURITY KEY
512
18
INTERNET
510
SENDER
512
SENDER'S SECURITY KEY
SESSION KEY
530

FIG. 4A

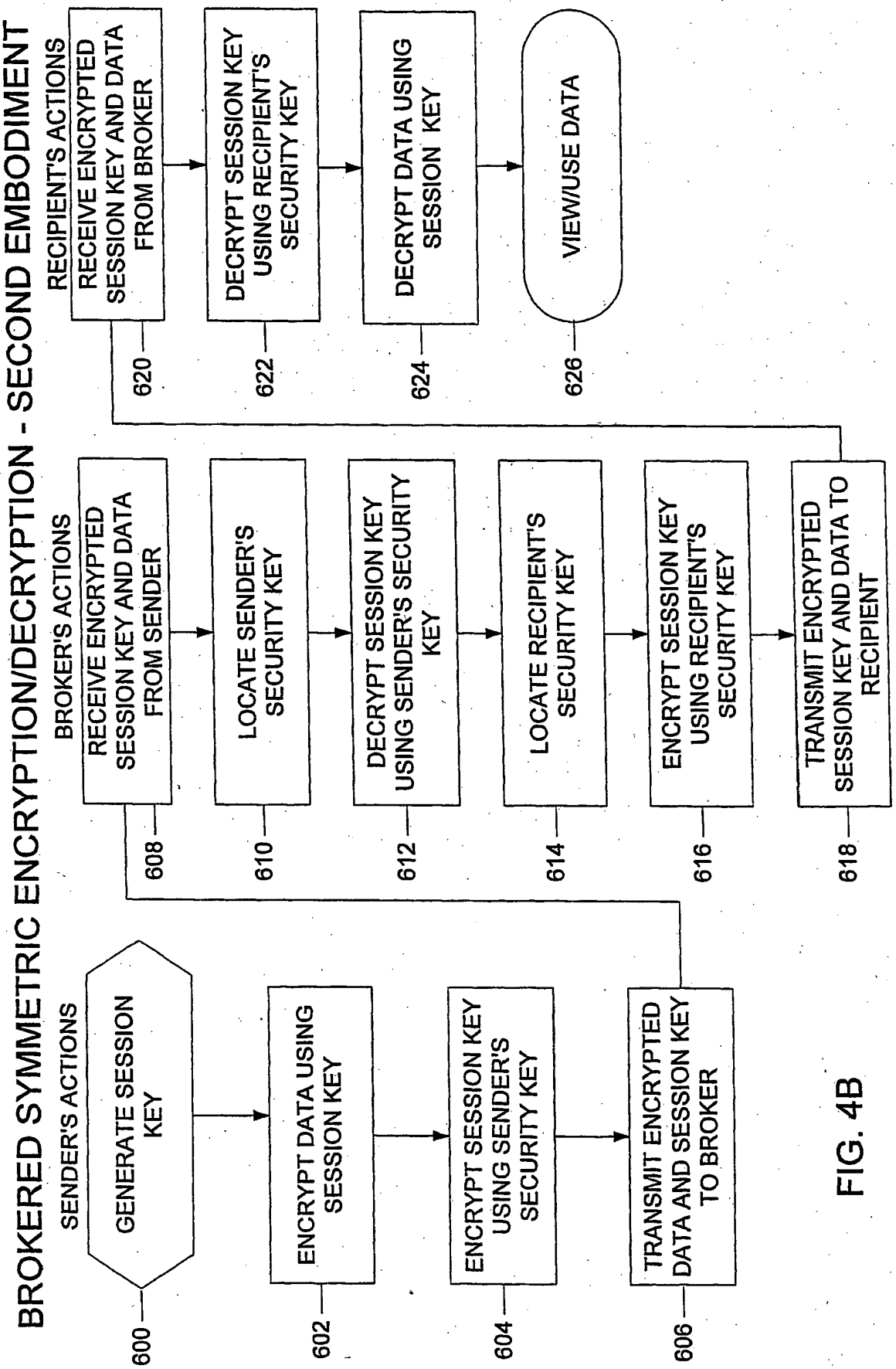
BROKERED SYMMETRIC ENCRYPTION/DECRYPTION - SECOND EMBODIMENT
SENDER'S ACTIONS
GENERATE SESSION KEY
600
ENCRYPT DATA USING SESSION KEY
602
ENCRYPT SESSION KEY USING SENDER'S SECURITY KEY
604
TRANSMIT ENCRYPTED DATA AND SESSION KEY TO BROKER
606
BROKER'S ACTIONS
RECEIVE ENCRYPTED SESSION KEY AND DATA FROM SENDER
608
LOCATE SENDER'S SECURITY KEY
610
DECRYPT SESSION KEY USING SENDER'S SECURITY KEY
612
LOCATE RECIPIENT'S SECURITY KEY
614
ENCRYPT SESSION KEY USING RECIPIENT'S SECURITY KEY
616
TRANSMIT ENCRYPTED SESSION KEY AND DATA TO RECIPIENT
618
RECIPIENT'S ACTIONS
RECEIVE ENCRYPTED SESSION KEY AND DATA FROM BROKER
620
DECRYPT SESSION KEY USING RECIPIENT'S SECURITY KEY
622
DECRYPT DATA USING SESSION KEY
624
VIEW/USE DATA
626

FIG. 4B

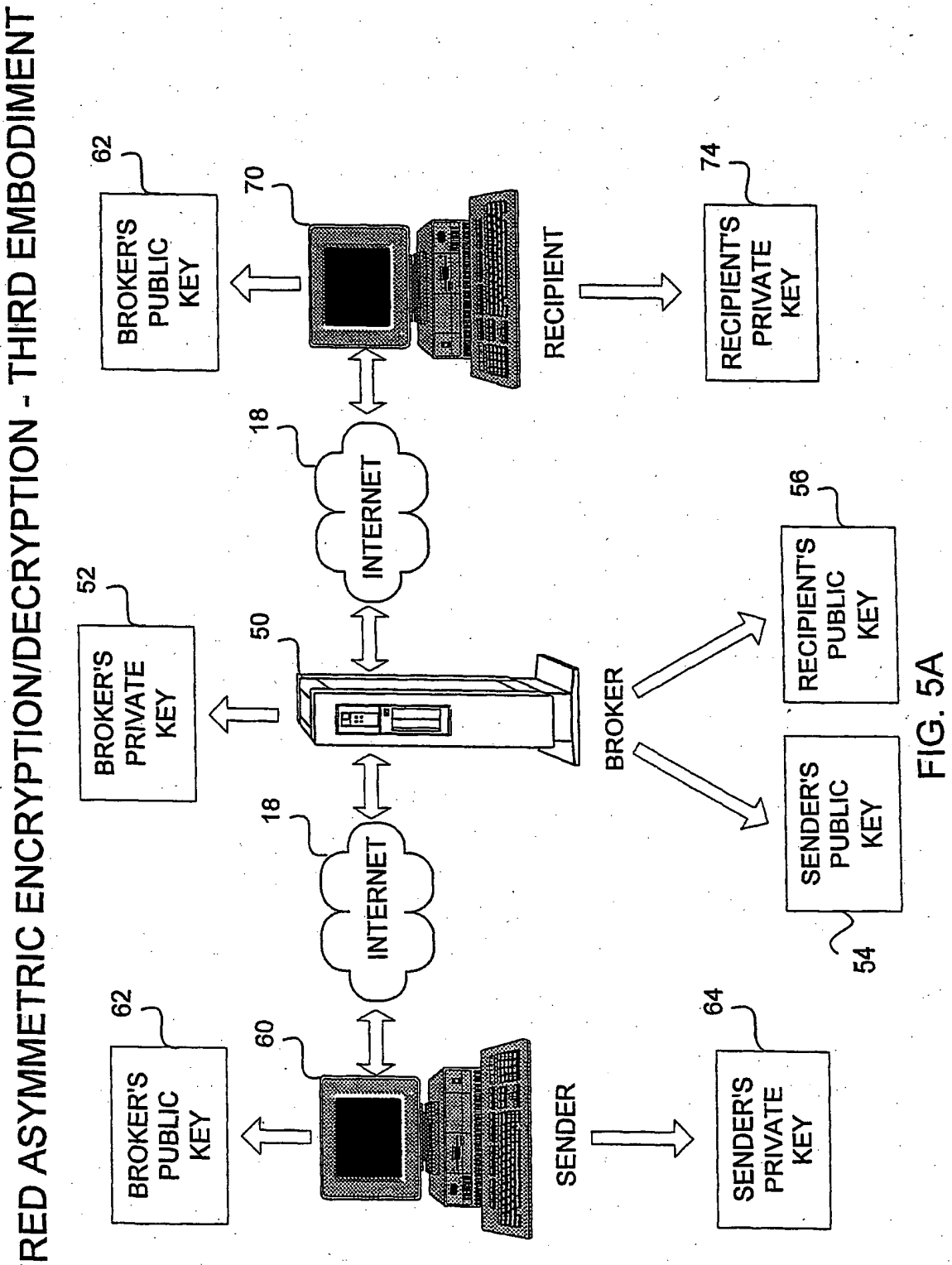
BROKERED ASYMMETRIC ENCRYPTION/DECRYPTION - THIRD EMBODIMENT
62
BROKER'S PUBLIC KEY
70
RECIPIENT
74
RECIPIENT'S PRIVATE KEY
18
INTERNET
52
BROKER'S PRIVATE KEY
50
BROKER
56
RECIPIENT'S PUBLIC KEY
SENDER'S PUBLIC KEY
54
18
INTERNET
62
BROKER'S PUBLIC KEY
60
SENDER
64
SENDER'S PRIVATE KEY

FIG. 5A

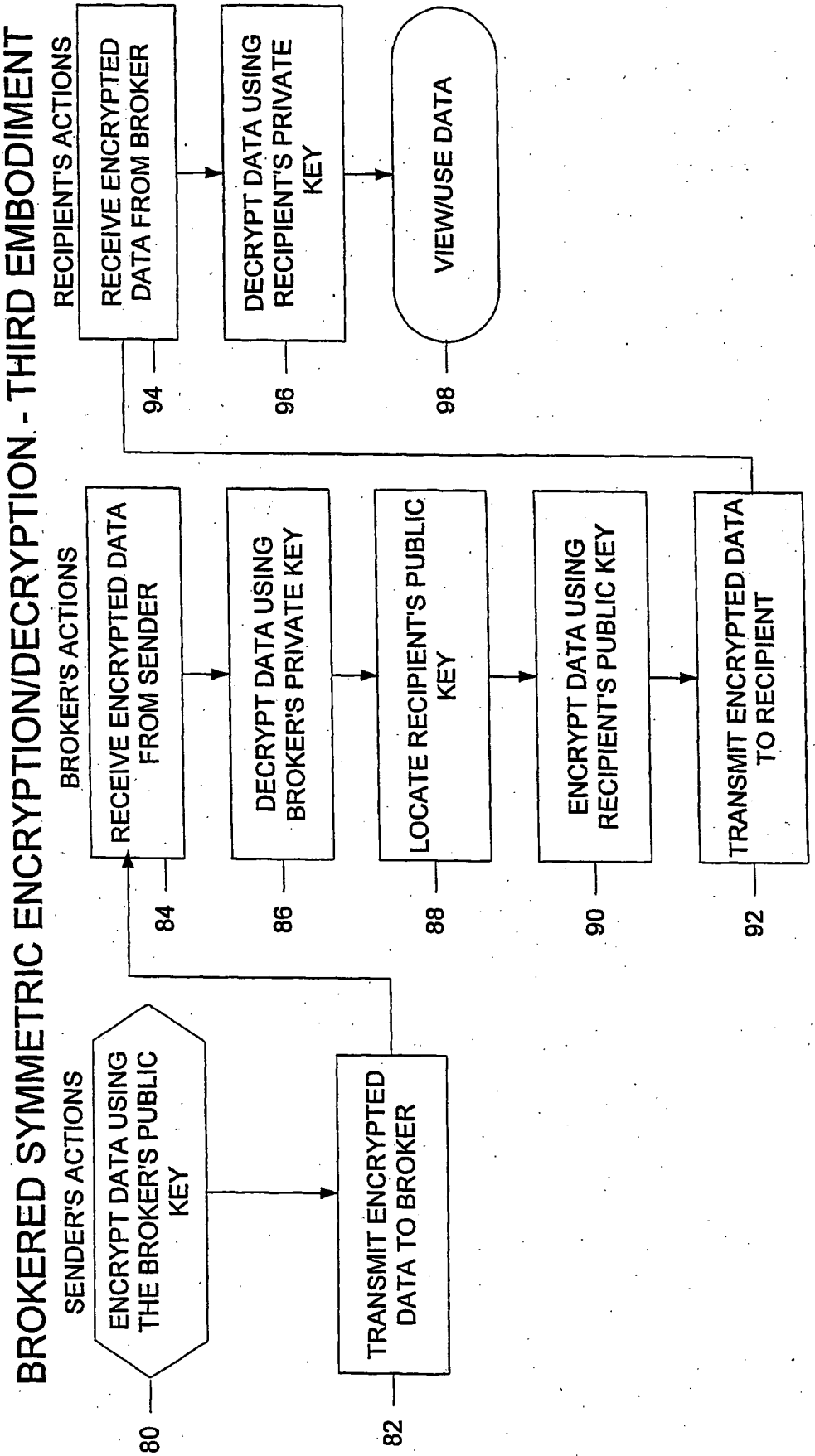
BROKERED SYMMETRIC ENCRYPTION/DECRYPTION - THIRD EMBODIMENT
SENDER'S ACTIONS
ENCRYPT DATA USING THE BROKER'S PUBLIC KEY
80
TRANSMIT ENCRYPTED DATA TO BROKER
82
BROKER'S ACTIONS
RECEIVE ENCRYPTED DATA FROM SENDER
84
DECRYPT DATA USING BROKER'S PRIVATE KEY
86
LOCATE RECIPIENT'S PUBLIC KEY
88
ENCRYPT DATA USING RECIPIENT'S PUBLIC KEY
90
TRANSMIT ENCRYPTED DATA TO RECIPIENT
92
RECIPIENT'S ACTIONS
RECEIVE ENCRYPTED DATA FROM BROKER
94
DECRYPT DATA USING RECIPIENT'S PRIVATE KEY
96
VIEW/USE DATA
98

FIG. 5B

BROKERED ASYMMETRIC ENCRYPTION/DECRYPTION - FOURTH EMBODIMENT

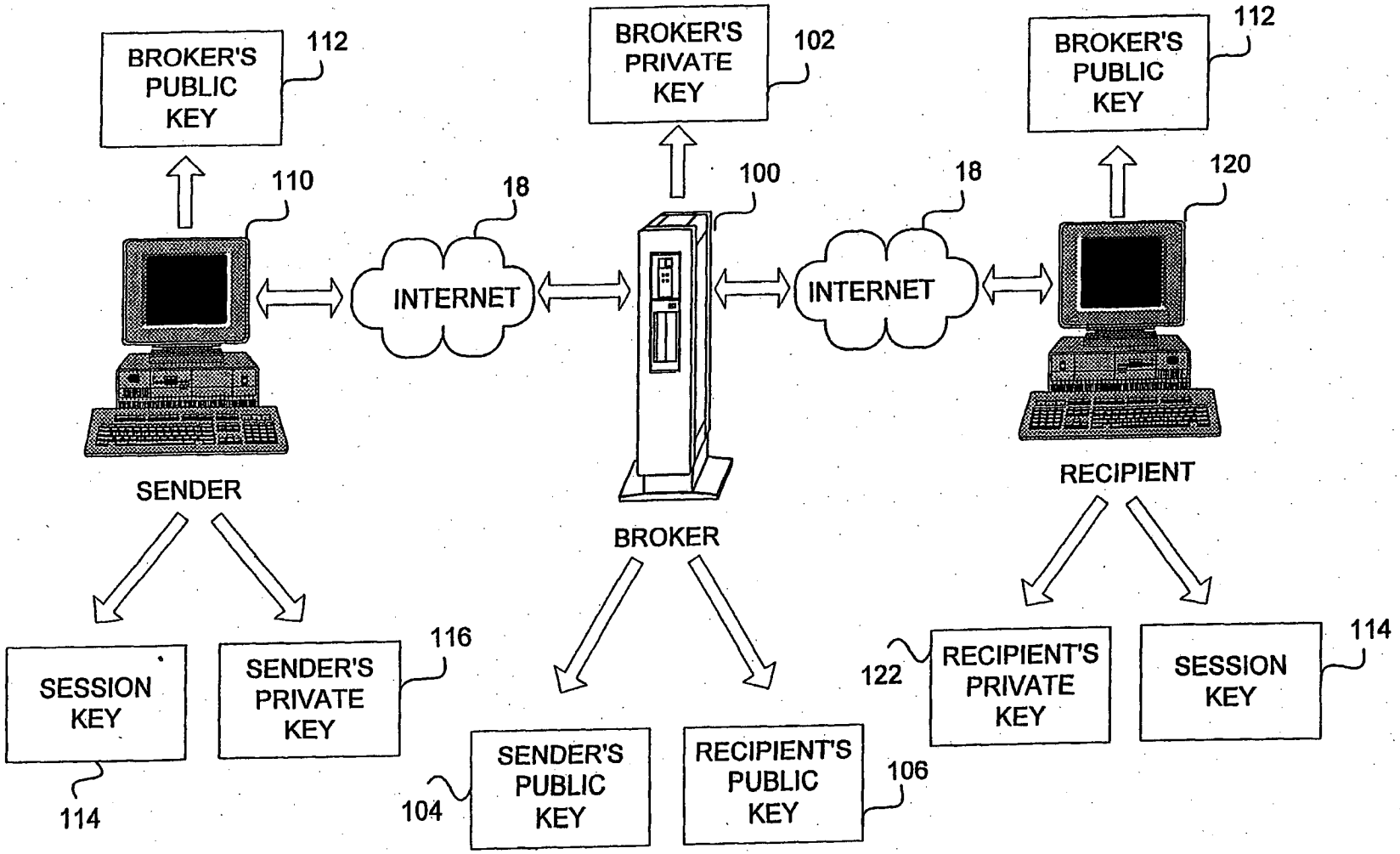

FIG. 6A

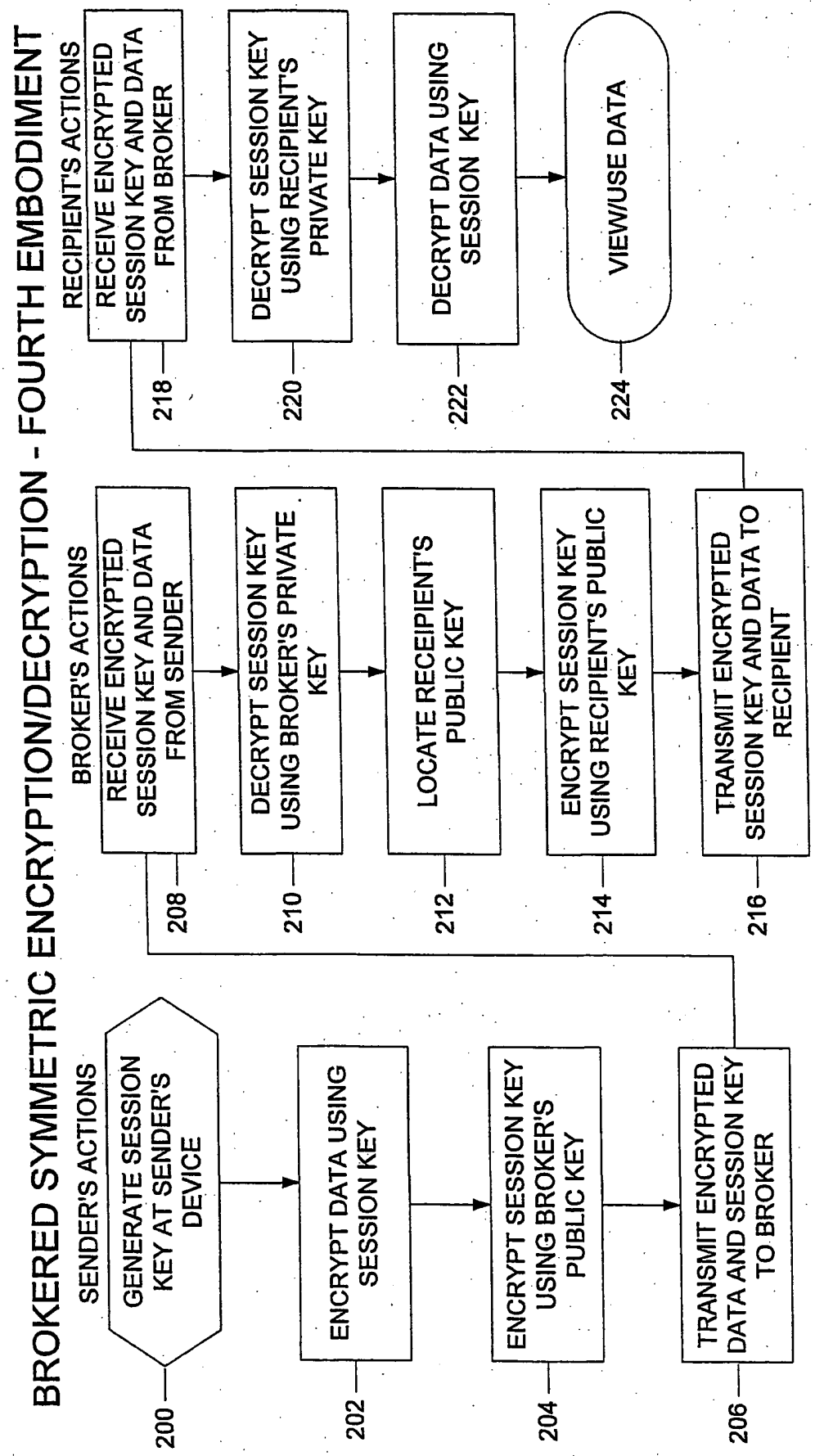
BROKERED SYMMETRIC ENCRYPTION/DECRYPTION - FOURTH EMBODIMENT
SENDER'S ACTIONS
GENERATE SESSION KEY AT SENDER'S DEVICE
200
ENCRYPT DATA USING SESSION KEY
202
ENCRYPT SESSION KEY USING BROKER'S PUBLIC KEY
204
TRANSMIT ENCRYPTED DATA AND SESSION KEY TO BROKER
206
BROKER'S ACTIONS
RECEIVE ENCRYPTED SESSION KEY AND DATA FROM SENDER
208
DECRYPT SESSION KEY USING BROKER'S PRIVATE KEY
210
LOCATE RECEIPIENT'S PUBLIC KEY
212
ENCRYPT SESSION KEY USING RECIPIENT'S PUBLIC KEY
214
TRANSMIT ENCRYPTED SESSION KEY AND DATA TO RECIPIENT
216
RECIPIENT'S ACTIONS
RECEIVE ENCRYPTED SESSION KEY AND DATA FROM BROKER
218
DECRYPT SESSION KEY USING RECIPIENT'S PRIVATE KEY
220
DECRYPT DATA USING SESSION KEY
222
VIEW/USE DATA
224

FIG. 6B